УДК 004.312.2:621.391.25:621.394.14(045)

[1] И.А.ЖУКОВ, [2] В.И.КУБИЦКИЙ

[1] Национальный авиационный университет, Киев
[2] Всероссийский научно-исследовательский институт радиоаппаратуры, Москва

ОЦЕНКА СЛОЖНОСТИ ВЫЧИСЛЕНИЙ В КОНЕЧНЫХ ПОЛЯХ

Аннотация. Приведен сравнительный анализ аппаратурной и временной сложности схем устройств, реализующих часто используемые методы вычислений в конечных полях.
Ключевые слова: коды, конечные поля, сложность схем устройств.
Анотація. Наведено порівняльний аналіз апаратурною та тимчасової складності схем пристроїв, що реалізують часто використовувані методи обчислень в кінцевих полях.
Ключові слова: коди, скінченні поля, складність схем пристроїв.
Abstract. The comparative analysis of the instrumental and temporal patterns of devices that implement commonly used methods of computation in finite fields.
Key words: codes, finite fields, the complexity of circuit’s devices.

Вступление

Вычисления в конечных полях находят применение во многих областях науки и техники (в теории кодирования, переключений, в криптографии, при цифровой обработке сигналов и др.).

Так как набор команд универсальных компьютеров не приспособлен для выполнения операций над элементами конечных полей, то для таких операций необходимо создавать дополнительные подпрограммы или специальные вычислительные устройства.

Актуальность

Вычисления в конечных полях с помощью вычислительных устройств могут быть реализованы различными способами. Наибольшее распространение получила реализация операций над многочленами и элементами конечных полей в линейных последовательностных машинах (регистрах сдвига). Можно применять методы с использованием логических функций, позволяющие реализовывать операции умножения, а также инвертирования в конечных полях малых порядков (со степенью порождающего поле многочлена ≤6), на комбинационных схемах. Используется также табличный метод, в соответствии с которым результаты операций в конечных полях хранятся в постоянном запоминающем устройстве (ПЗУ) или программируемой логической матрице (ПЛМ). Основу аппаратной реализации могут составить специальные конечные автоматы, специализированные процессоры с микропрограммным управлением и систолические структуры.

Цель

Цель статьи состоит в том, чтобы получить соотношения сложности схем, которые бы позволяли выбирать лучшие из разработанных или известных методов и схем по необходимым параметрам (аппаратурным затратам, времени вычисления).

Под аппаратурной сложностью (N) схемы будем понимать количество функциональных элементов базисного набора (схем И с двумя входами, схем ИЛИ с двумя входами и схем НЕ) в схеме, реализующей заданную функцию.

Под временной сложностью (Т) схемы будем понимать время, необходимое для реализации схемой заданной функции; при этом за единицу времени принимается время срабатывания элемента базисного набора (t).

Задачи

Сложность схем выполнения операций с многочленами над полем GF(2)

Операции выполняются с многочленами

$$\begin{aligned} a(x) &= a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \ldots + a_1 x + a_0; \\ b(x) &= b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_1 x + b_0, \end{aligned} \qquad (1)$$

где a_i, $b_j \in GF(2)$.

Сложность схем умножения многочленов.

Сложность схем умножения приведем для случая, когда $\deg a(x) = \deg b(x) = m - 1$.

Сложность схемы умножения многочленов на сдвиговых регистрах (ССУМ) [1, 2] равна (при наличии регистра для записи и хранения одного из сомножителей в ССУМ):

$$N_{ССУМ} = 34m - 23;$$
$$T_{ССУМ} = (40m - 29)t.$$

Сложность комбинационной схемы умножения многочленов (КСУМ), реализующей предложенный метод непосредственного умножения многочленов [3], составляет:

$$N_{КСУМ} = m(5m - 8) + 4;$$
$$T_{КСУМ} = (3m - 2)t.$$

Сложность схем деления многочленов.

Деление многочлена $c(x)$ на многочлен $a(x)$ производится в соответствии с выражением

$$c(x) = a(x) \cdot b(x) + r(x),$$

где многочлены $a(x)$ и $b(x)$ представлены выражениями (1), многочлен $r(x) = r_{r-1}x^{r-1} + r_{r-2}x^{r-2} + \ldots + r_1x + r_0$ является остатком от деления, коэффициенты a_i, b_j, $r_s \in$ GF(p).

Степень многочлена $c(x)$ (делимого) равна:

$$\deg c(x) = (d-1) = \deg a(x) + \deg b(x) = (m-1) + (n-1).$$

Степень многочлена $b(x)$ (частного) изначально неизвестна, но ее можно вычислить из выражения:

$$\deg b(x) = (n-1) = \deg c(x) - \deg a(x) = (d-1) - (m-1).$$

Степень многочлена $r(x)$ (остатка) определяется степенью делителя $a(x)$:

$$\deg r(x) = (r-1) < \deg a(x),$$

поэтому $\deg r(x) < (m-1)$.

Сложность схемы деления многочленов на сдвиговых регистрах (ССДМ) [1, 2, 4] равна (при наличии регистра для записи и хранения делителя $a(x)$):

$$N_{ССДМ} = 34m - 33;$$
$$T_{ССДМ} = (20d + 7)t.$$

Сложность комбинационной схемы деления многочленов (КСДМ) и универсальной КСДМ (УКСДМ) [5], реализующих предложенный в [6] метод непосредственного деления многочленов, составляет:

$$N_{КСДМ} = N_{УКСДМ} = 5(m-1)(d-m+1);$$
$$T_{КСДМ} = T_{УКСДМ} = 4(d-m+1)t.$$

Сложность схем выполнения операций над элементами конечного поля GF(2^M)

Сложность схем приводится для любого образующего конечное поле неприводимого многочлена $p(x)$ заданной степени m и без учета сложности регистра для хранения этого многочлена.

Сложность схем умножения элементов конечного поля.

Сложность схемы умножения элементов конечного поля на сдвиговых регистрах (ССУЭ) [4] равна:

$$N^{И}_{ССУЭ} = 77m - 2;$$
$$T^{И}_{ССУЭ} = (22m + 15)t.$$

Схема, реализующая умножение по методу Барти–Шнайдера [7] (схема БШУЭ), имеет аппаратурную сложность (для вычисления всех величин c_i и без учета сложности вычисления величин $\alpha^{(i)}_{kl}$; схема вычисления величин $\alpha^{(i)}_{kl}$ и ее сложность в публикациях не приводятся):

$$N^{И}_{БШУЭ} = (m + 1)(5m - 4)m.$$

Время умножения составляет (при одновременном вычислении величин c_i и с учетом времени вычисления на схемах И величин ($a_j \cdot \alpha^{(i)}_{kl}$)):

$$T^{И}_{БШУЭ} = (6m - 4)t.$$

В [8] разработан метод непосредственного умножения элементов конечного поля GF(2^M). Сложность комбинационных схем [9] для реализации этого метода составляет (без учета сложности вычисления операционных коэффициентов $p^{(j)}_i$ и их хранения):

$$N^{И}_{КСУЭ} = m(10m - 13) + 4;$$
$$T^{И}_{КСУЭ} = (3m + 2)t.$$

Для разработанного в [10] метода умножения элементов конечного поля GF(2^M) с использованием умножения и деления многочленов над полем GF(2) сложность комбинационной схемы умножения (КСУЭ) равна:

$$N_{КСУЭ} = m(10m - 13) + 4;$$
$$T_{КСУЭ} = (6m - 5)t.$$

Сложность схем инвертирования элементов конечного поля.

Комбинационные схемы инвертирования элементов конечного поля GF(2^M) с вычислением миноров (КСИЭ-М), реализующие разработанный в [11] метод, имеют сложность:

$$N_{КСИЭ-М} = (5m^2 - 4m)(m - 1)/2 + \sum_{r=2}^{m-1}(5r - 4)[m!/r!(m - r)!];$$
$$T_{КСИЭ-М} = (m - 1)(3m + 4)t/2.$$

Инвертирование элементов конечного поля можно выполнять по методу Барти–Шнайдера [7]. Однако, схемы инвертирования, реализующих этот метод (схемы БШИЭ), и их сложность в публикациях не приводится. В [12] разработана схема вычисления одного элемента $\hat{A}_{i+1,1}$ матрицы $\hat{A}$ для схем БШИЭ. Сложность схемы для одновременного вычисления всех элементов составляет:

$$\hat{N}_{БШИЭ} = (5m - 4)m^2;$$
$$\hat{T}_{БШИЭ} = (3m - 2)t.$$

Решение задачи

Сравнение сложности схем вычислений в конечных полях

Сравнение сложности схем выполнения операций с многочленами над полем GF(2).
В результате сравнения КСУМ и ССУМ получаем:

$$\Delta N = N_{ССУМ} - N_{КСУМ} = (42 - 5m)m - 27;$$
$$\Delta T = T_{ССУМ} - T_{КСУМ} = (37m - 27)t.$$

На рис. 1 и рис. 2 приведены графики сложностей КСУМ и ССУМ, из которых видно, что временная сложность КСУМ всегда меньше временной сложности ССУМ, а аппаратурная сложность КСУМ меньше сложности ССУМ для $m \le 7$.
Сравнение КСДМ и ССДМ дает:

$$\Delta N = N_{ССДМ} - N_{КСДМ} = (m-1)[34 - 5(d - m + 1)] + 1;$$
$$\Delta T = T_{ССУМ} - T_{КСУМ} = (16d + 4m + 3)t.$$

Приведенные на рис. 3 и рис. 4 графики показывают, что временная сложность КСДМ (УКСДМ) всегда меньше временной сложности ССДМ, аппаратурная сложность – меньше для определенных соотношений степеней делимого $c(x)$ и делителя $a(x)$.

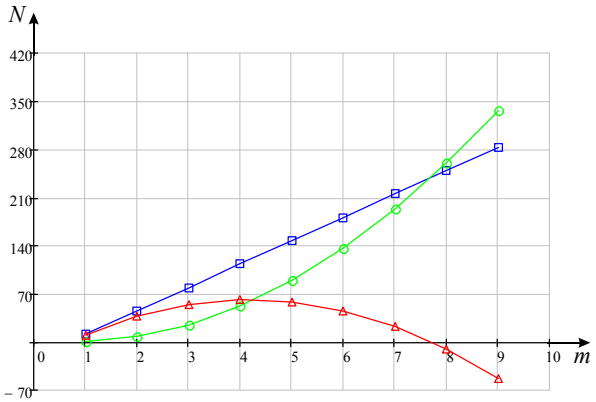

Рисунок 1 – График аппаратурной сложности ССУМ и КСУМ:
– NССУМ, – NКСУМ, – ΔN

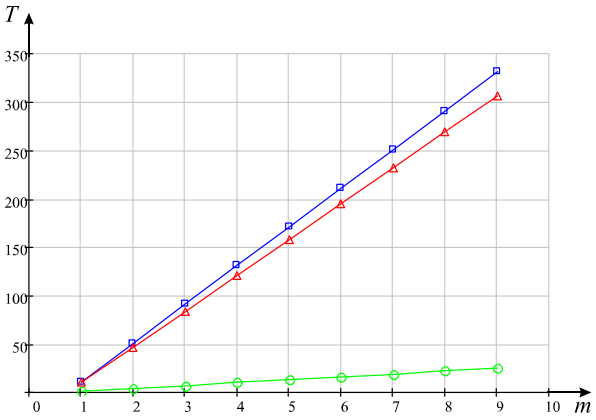

Рисунок 2 – График временной сложности ССУМ и КСУМ:
– TССУМ, – TКСУМ, – ΔT

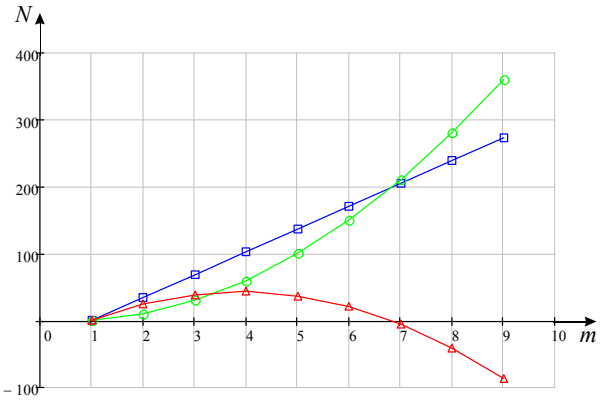

Рисунок 3 – График аппаратурной сложности ССДМ и КСДМ (УКСДМ):
– NССДМ, – NКСДМ, – ΔN

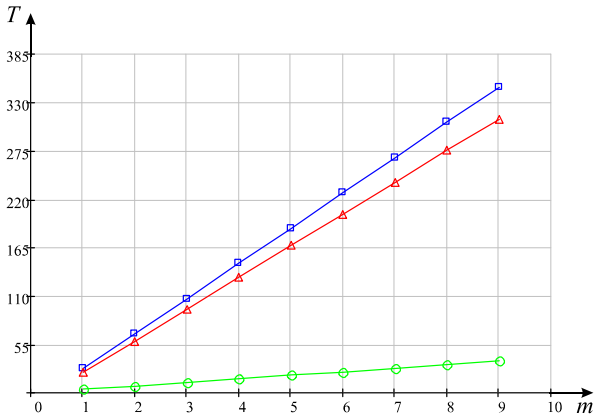

Рисунок 4 – График временной сложности ССДМ и КСДМ (УКСДМ):
– TССДМ, – TКСДМ, – ΔT

Сравнение сложности схем выполнения операций над элементами конечного поля GF(2^M).
Сравнивая КСУЭ с ССУЭ, имеем:

$$\Delta N = N^{И}_{ССУЭ} - N_{КСУЭ} = 2(45m - 5m^2 - 3);$$

$$\Delta T = T^{И}_{ССУЭ} - T_{КСУЭ} = (16m + 20)t.$$

Временная сложность КСУЭ всегда меньше временной сложности ССУЭ, а аппаратурная сложность КСУЭ меньше сложности ССУЭ для $m \le 8$. На рис. 5 и рис. 6 представлены графики сложностей КСУЭ и ССУЭ.

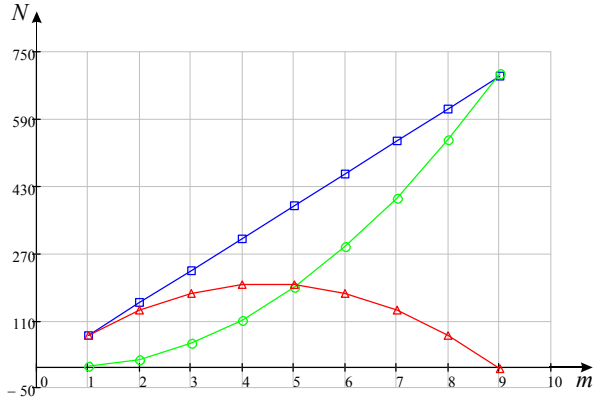

Рисунок 5 – График аппаратурной сложности ССУЭ и КСУЭ:
– NССУЭ, – NКСУЭ, – ΔN

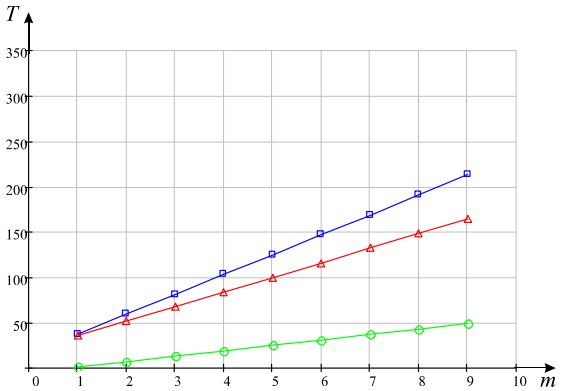

Рисунок 6 – График временной сложности ССУЭ и КСУЭ:
– ТССУЭ, – ТКСУЭ, – ΔТ

Сравнивая КСУЭ с БШУЭ, получаем минимальные значения величин (т.к. схема вычисления величин $\alpha_{kl}^{(i)}$ и ее сложность в публикациях не приводятся):

$$\Delta N^{min} = N^{И}_{БШУЭ} - N_{КСУЭ} = m[m(5m-9)+9]-4; \quad \Delta T^{min} = T^{И}_{БШУЭ} - T_{КСУЭ} = t.$$

Таким образом, сложность КСУЭ всегда меньше сложности БШУЭ.

Точное сравнение КСИЭ-М и схем БШИЭ выполнить невозможно, так как не известны аппаратурная и временная сложности схем вычисления элементов $\alpha_{kl}^{(i)}$ матрицы M_i и схем вычисления минора $\hat{M}_{i+1,1}$ элемента $\hat{A}_{i+1,1}$ матрицы $\hat{A}$ в схемах БШИЭ (обозначения приведены в [12]). Однако можно определить величины сложностей этих схем, при которых КСИЭ-М будут лучше схем БШИЭ.

Если принять во внимание, что аппаратурные сложности схем вычисления минора $\hat{M}_{i+1,1}$ элемента $\hat{A}_{i+1,1}$ матрицы $\hat{A}$ в схемах БШИЭ и минора M_{1j} элемента A_{1j} матрицы A в КСИЭ-М (обозначения приведены в [12]) одинаковы, то в результате сравнения КСИЭ-М и схем БШИЭ получим:

$$\Delta N^{min} = N^{min}_{БШИЭ} - N_{КСИЭ-М} = m(5m^2+m-4)/2.$$

Поэтому аппаратурная сложность КСИЭ-М всегда меньше аппаратурной сложности схем БШИЭ. Это при том, что не учтена сложность схемы для вычисления элементов $\alpha_{kl}^{(i)}$ матрицы M_i в схемах БШИЭ (такая схема и ее сложность в публикациях отсутствуют). При этом временная сложность $T_{КСИЭ-М} \le T_{БШИЭ}$, если временная сложность схем вычисления элементов $\alpha_{kl}^{(i)}$ матрицы M_i в схемах БШИЭ будет не менее величины $(m-2)t$.

На рис. 7 показан график аппаратурной сложности БШИЭ и КСИЭ-М.

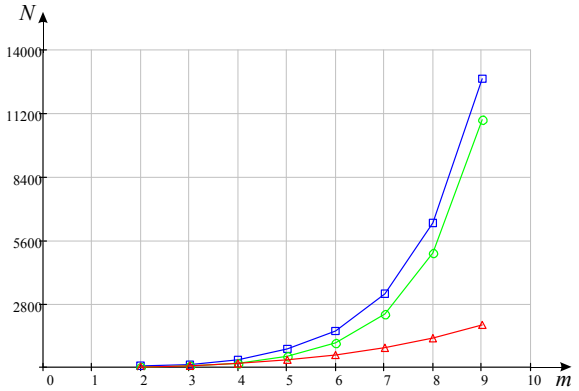

Рисунок 7 – График аппаратурной сложности БШИЭ и КСИЭ-М:
– NБШИЭ, – NКСИЭ-М, – ΔN

Здесь:

$$N_{БШИЭ} = N^{min}_{БШИЭ} = (5m^2 - 4m)(m-1)/2 + \sum_{r=2}^{m-1}(5r-4)[m!/r!(m-r)!] + m(5m^2 + m - 4)/2.$$

Выводы

Полученные в результате сравнения соотношения сложностей схем, реализующих разработанные и известные методы вычислений в конечных полях, позволяют выбирать лучшие из этих методов и схем по необходимым параметрам (аппаратурным затратам, времени вычисления) [13].

Комбинационные схемы, реализующие новые методы вычислений в конечных полях, значительно сокращают время вычислений по сравнению с реализацией в линейных последовательностных машинах: в 13 раз – для операций умножения многочленов, в 9 раз – для операций деления многочленов, в 4 раза – для операций умножения элементов конечного поля.

Для некоторых степеней многочленов над полем GF(2), с которыми производятся операции, а также степеней образующего поле $GF(2^M)$ неприводимого примитивного многочлена $p(x)$ разработанные схемы также лучше с точки зрения аппаратурной сложности. Эти схемы имеют преимущество по сложности перед другими известными комбинационными схемами, например, реализующими метод Барти–Шнайдера.

Список литературы

1. Гилл А. Линейные последовательностные машины / Гилл А.; пер. с англ. Бернштейна А.С.; под ред. Цыпкина Я.З. – М.: Наука, 1974. – 287 с.

2. Питерсон У. Коды, исправляющие ошибки / Питерсон У., Уэлдон Э.; пер. с англ.; под ред. Добрушина Р.Л. и Самойленко С.И. – М.: Мир, 1976. – 596 с.

3. Кубицкий В.И. Операции над многочленами в поле GF(2) / Кубицкий В.И. // Науч. вестн. ГосНИИ “Аэронавигация”. – 2007. – №7. – С. 185-194.

4. Блох Э. Л. Обобщенные каскадные коды (Алгебраическая теория и сложность реализации) / Блох Э.Л., Зяблов В.В. – М.: Связь, 1976. – 240 с.

5. Пат. №40145 Украина, МПК (2009) G06F 7/00. Пристрій для ділення елементів скінченних полів GF(2n) / Жуков И.А., Кубицкий В.И., Синельников А.А.; патентообладатель Нац. авиац. ун-т. – № u 2008 12736; заявл. 30.10.2008; опубл. 25.03.2009, Бюл. №6.

6. Кубицкий В.И. Деление многочленов над полем GF(2) / Кубицкий В.И. // Науч. вестн. МГТУ ГА. – 2008. – № 132 (8). – С. 86-93.

7. Bartee T.C. Computations with finite fields / Bartee T.C., Shneider D.I. // Information and Control. – 1963. – Vol. 6. – P. 79-98.

8. Жуков И.А. Алгоритмы выполнения операций над элементами конечного поля $GF(2^M)$ в вычислительных устройствах / Жуков И.А., Кубицкий В.И., Дрововозов В.И. // Авіа-2007: VIII Міжнар. наук.-техн. конф., 25–27 квітня 2007 р.: матеріали конф. – К., 2007. – Т.1. – С. 13.5-13.8.

9. Пат. №43629 Украина, МПК (2009) H03M 7/00. Пристрій для множення елементів скінченних полів GF(2n) / Жуков И.А., Кубицкий В.И., Синельников А.А.; патентообладатель Нац. авиац. ун-т. - № u 2009 02754; заявл. 25.03.2009; опубл. 25.08.2009, Бюл. №16.

10. Кубицкий В. И. Умножение элементов конечного поля $GF(2^M)$ / Кубицкий В.И. // Науч. вестн. МГТУ ГА. – 2009. – №145 (8). – С. 105-112.

11. Кубицкий В. И. Организация мультипликативного обращения элементов конечного поля / Кубицкий В.И. // Проблеми інформатизації та управління: зб. наук. пр. – 2010. – Вип. 1 (29). – С. 111-117.

12. Кубицкий В.И. Методы инвертирования элементов конечного поля и сложность их реализации / Кубицкий В. И. // Науч. вестн. ГосНИИ “Аэронавигация”: сб. науч. тр. – 2010. – №10. – С. 116-126.

13. Жуков И.А. Сложность реализации вычислений в конечных полях / Жуков И.А. Кубицкий В.И. // Комп’ютерні системи та мережні технології (CSNT-2013): Зб. тез VI Міжнар. наук.-технічн. конф. – Київ, 2013. – С. 43.

Статья поступила: 28.05.2013.

Відомості про авторів

Жуков Игорь Анатольевич, д.т.н., профессор, заведующий кафедры компьютерных систем и сетей Национального авиационного университета.

Кубицкий Валерий Иванович, к.т.н., заместитель директора Всероссийского научно-исследовательского института радиоаппаратуры.